Microsoft

hypothesis

ดัชนีความปลอดภัยของข้อมูล

แนวโน้ม ข้อมูลเชิงลึก และกลยุทธ์
ในการรักษาความปลอดภัยข้อมูล

คำนำ

ในช่วงเวลาที่ข้อมูลเพิ่มขึ้นอย่างรวดเร็ว เป็นที่แน่ชัดมากขึ้นว่าข้อมูลขององค์กรนั้นไม่ได้สำคัญน้อยไปกว่าส่วนอื่นๆ ที่สำคัญขององค์กรเลย ความมั่งคั่งของข้อมูลที่สร้างและใช้โดยองค์กรต่างๆ ช่วยเพิ่มประสิทธิภาพให้กับการดำเนินงานที่สำคัญ มอบการตัดสินใจเชิงกลยุทธ์และเป็นสากล และสร้างความเป็นไปได้สำหรับอนาคตขององค์กร ข้อมูลไม่ได้เป็นเพียงทรัพยากร แต่เป็นหัวใจสำคัญขององค์กรยุคใหม่

ซึ่งด้วยการพึ่งพาข้อมูลที่เพิ่มขึ้นนี้ ความจริงอย่างหนึ่งก็คือช่องโหวในเงาดิจิทัลนั้นมีอยู่จริงและขยายตัวอย่างรวดเร็ว ภัยคุกคามทางไซเบอร์ การละเมิดข้อมูล และเหตุการณ์ความเสี่ยงจากภายในไม่ใช่เรื่องที่เกิดขึ้นได้ยากอีกต่อไป แต่กลับแพร่หลายและทวีความรุนแรงขึ้น ก่อให้เกิดความเสี่ยงต่อองค์กรที่ต้องพึ่งพาข้อมูล ในบรรดาผู้มีอำนาจตัดสินใจที่เราสำรวจเมื่อเร็วๆ นี้ 89% กล่าวว่าพวกเขามองว่ามาตรการรักษาความปลอดภัยข้อมูลของตนมีความสำคัญต่อความสำเร็จโดยรวม

ในเอกสารไวท์เปเปอร์นี้ เราเริ่มดำเนินการสำรวจความจำเป็นพื้นฐานดังกล่าว ซึ่งก็คือการปกป้องข้อมูลขององค์กรคุณ ฉันและทีมรู้สึกตื่นเต้นที่จะมาแชร์สิ่งที่เราค้นพบกับคุณและหวังว่าจะได้เริ่มการสนทนาเกี่ยวกับวิธีผลักดันการรักษาความปลอดภัยข้อมูลไปสู่ความเป็นเลิศร่วมกันต่อไป การเรียนรู้ของเราเป็นตัวอย่างว่าการรักษาความปลอดภัยข้อมูลอยู่ในช่วงหัวเลี้ยวหัวต่อที่สำคัญอย่างไร พร้อมกับที่ผู้มีอำนาจตัดสินใจด้านความปลอดภัยเห็นพ้องกันว่าสิ่งนี้จำเป็นต่อความปลอดภัยข้อมูลของตน และส่วนใหญ่บอกว่าพวกเขามั่นใจในสิ่งที่พวกเขากำลังทำอยู่ พวกเขากำลังประสบกับการรักษาความปลอดภัยข้อมูล เหตุการณ์ และความท้าทายจำนวนมากมายไปพร้อมๆ กัน และ 80% ของผู้นำที่เราพูดคุยด้วยตระหนักดีว่าแนวทางแบบผสานรวมของชุดโปรแกรมรวมนั้นเหนือกว่าโซลูชันเฉพาะจุด แต่บริษัทส่วนใหญ่ยังคงใช้ระบบเครื่องมือที่หลากหลายและกระจัดกระจายเพื่อปกป้องข้อมูลของตน ซึ่งมักจะส่งผลให้มีเหตุการณ์ด้านความปลอดภัยมากขึ้น แทนที่จะลดน้อยลง

เรายินดีให้คุณได้อ่านและแชร์รายงานล่าสุดนี้ และถือเป็นจุดเริ่มต้นของการสนทนาครั้งใหม่กับทีมของเราเกี่ยวกับวิธีที่เราจะช่วยรักษาอนาคตที่มีร่วมกันของเราได้ดีที่สุด

Rudra Mitra

รองประธาน

Microsoft Data Security and Compliance

ข้อมูลเบื้องต้น

การป้องกันการละเมิดข้อมูลและเหตุการณ์ด้านความปลอดภัยอื่นๆ ยังคงเป็นข้อกังวลอย่างต่อเนื่องสำหรับผู้มีอำนาจตัดสินใจด้านความปลอดภัยและความเสี่ยง และเป็นรากฐานสำคัญของโปรแกรมความปลอดภัยทางไซเบอร์ เนื่องจากการละเมิดเพียงครั้งเดียวอาจทำให้เกิดความเสียหายต่อชื่อเสียงและการเงินอย่างมีนัยสำคัญ องค์กรต่างๆ ได้รับมอบหมายให้ปกป้องข้อมูลที่ละเอียดอ่อนมากมาย รวมถึงข้อมูลพนักงานและลูกค้า ทรัพย์สินทางปัญญา การคาดการณ์ทางการเงิน และข้อมูลการปฏิบัติงาน

เพื่อทำความเข้าใจแนวทางปฏิบัติและแนวโน้มด้านความปลอดภัยข้อมูลในปัจจุบัน ตลอดจนระบุโอกาสสำหรับองค์กรในการปรับปรุงความปลอดภัยข้อมูล Microsoft จึงมอบหมายให้หน่วยงานวิจัยอิสระ Hypothesis Group ดำเนินการสำรวจในหมู่ผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลนานาชาติมากกว่า 800 ราย ซึ่งรายงานนี้จะนำเสนอข้อค้นพบที่สำคัญ 5 ประการจากการวิจัย รวมถึงแนวโน้มข้อมูลเชิงลึก และกลยุทธ์ในการรักษาความปลอดภัยข้อมูล

ประเด็นสำคัญ

1

ผู้มีอำนาจตัดสินใจคิดว่าตนเองได้รับการปกป้อง แต่ความเป็นจริงกลับไม่สอดคล้องกับการรับรู้

แม้ว่าผู้มีอำนาจตัดสินใจส่วนใหญ่กล่าวว่าพวกเขาพอใจและมั่นใจกับโซลูชันการรักษาความปลอดภัยข้อมูล แต่พวกเขายังคงประสบปัญหาด้านความปลอดภัยข้อมูลโดยเฉลี่ย 59 ครั้งต่อปี ซึ่งเป็นผลกระทบที่มีค่าใช้จ่ายสูง

2

การมีเครื่องมือมากขึ้นไม่ได้หมายความว่ามีความปลอดภัยหรือประสิทธิภาพของข้อมูลมากขึ้น แต่เป็นสิ่งที่ตรงกันข้าม

80% ของผู้มีอำนาจตัดสินใจยอมรับว่าโซลูชันแบบผสานรวมที่ครบวงจรนั้นเหนือกว่าโซลูชันแบบแมนวลที่ดีที่สุดเสียอีก แต่แนวทางขององค์กรในการใช้เครื่องมือยังคงกระจัดกระจาย โดยใช้เครื่องมือรักษาความปลอดภัยข้อมูลโดยเฉลี่ยมากกว่า 10 รายการ แต่บริษัทที่มีเครื่องมือมากที่สุดก็ประสบปัญหาด้านความปลอดภัยข้อมูลมากขึ้นเช่นกัน ซึ่งบ่งชี้ว่ายิ่งเครื่องมือมีการกระจัดกระจายมากขึ้นเท่าใด การรักษาความปลอดภัยก็จะยิ่งอ่อนแอลงเท่านั้น

3

องค์กรต่างๆ ยังคงต้องเผชิญกับความเครียดจากเหตุการณ์ด้านความปลอดภัยข้อมูลทั้งภายนอกและภายใน โดยเฉพาะอย่างยิ่งข้อมูลทางธุรกิจ

50% ขององค์กรที่สำรวจเคยประสบกับการโจมตีด้วยแรนซัมแวร์หรือมัลแวร์ในปีที่ผ่านมา และผู้มีอำนาจตัดสินใจจำนวนมากไม่เชื่อว่าองค์กรของตนพร้อมอย่างเต็มที่ในการป้องกันและจัดการกับปัญหาในอนาคต บุคคลภายในที่ประสงค์ร้ายถือเป็นข้อกังวลอันดับต้นๆ นอกจากนี้ องค์กรต่างๆ ยังมีความกังวลอย่างมากเกี่ยวกับช่องโหว่ของข้อมูลทางธุรกิจของตน เป็นการตอกย้ำอีกครั้งหนึ่งถึงความต้องการแพลตฟอร์มความปลอดภัยที่จัดการความเสี่ยงอย่างครอบคลุม

ประเด็นสำคัญ

4

องค์กรต่างๆ ต้องการระบบคลาวด์และ AI เพื่อขับเคลื่อนการเปลี่ยนแปลงทางดิจิทัล แต่ก็เป็นจุดที่ข้อมูลที่มีความเสี่ยงมากที่สุดเช่นกัน

แอปพลิเคชันระบบคลาวด์และเทคโนโลยี AI กลายเป็นสิ่งจำเป็นสำหรับการทำงานร่วมกันและประสิทธิภาพการทำงานขององค์กร อย่างไรก็ตาม การพัฒนานี้ยังทำให้เกิดความเสี่ยงแบบไดนามิกและหลายแง่มุมมากขึ้น ในขณะที่องค์กรต่างๆ หันมาใช้ AI ทำให้การยกระดับความปลอดภัยข้อมูลเพื่อให้สามารถใช้งานอย่างมีความรับผิดชอบและปลอดภัยจึงกลายเป็นเรื่องสำคัญ

5

ระบบอัตโนมัติและ AI จึงเป็นแนวทางในการปกป้องที่ดียิ่งขึ้น

องค์กรต่างๆ ต้องการให้ทีมของตนใช้เวลาในการตรวจจับน้อยลงและมีเวลาในการป้องกันมากขึ้น ระบบอัตโนมัติช่วยให้ทีมมุ่งเน้นไปที่มาตรการเชิงรุกได้มากขึ้น ในขณะที่การใช้ AI เพื่อรักษาความปลอดภัยข้อมูลก็ช่วยให้องค์กรมีกลยุทธ์และชาญฉลาดมากขึ้นเกี่ยวกับภัยคุกคามในอนาคต

1

ผู้มีอำนาจตัดสินใจคิดว่าตนเองได้รับการปกป้อง แต่ความเป็นจริงกลับไม่สอดคล้องกับการรับรู้

ผู้มีอำนาจตัดสินใจคิดว่าตนเองได้รับการปกป้อง แต่ความเป็นจริงกลับไม่สอดคล้องกับการรับรู้

โดยภายนอก ผู้มีอำนาจตัดสินใจคาดการณ์ถึงความมั่นใจและความพึงพอใจในระดับสูงต่อโซลูชันการรักษาความปลอดภัยข้อมูล องค์กรส่วนใหญ่ยอมรับว่าการควบคุมความปลอดภัยข้อมูลของตนนั้นเพียงพอแล้วในการป้องกันไม่ให้ข้อมูลถูกละเมิด พวกเขารู้สึกว่าตนเองรู้ข้อมูลส่วนใหญ่อยู่ที่ใด และพวกเขาสามารถตรวจจับความเสี่ยงส่วนใหญ่เกี่ยวกับข้อมูลได้

ในขณะเดียวกัน องค์กรต่างๆ ยังคงเผชิญกับเหตุการณ์ด้านความปลอดภัยข้อมูลจำนวนมาก โดยเฉลี่ย 59 เหตุการณ์ในช่วง 12 เดือนที่ผ่านมา โดย 1 ใน 5 ของเหตุการณ์ดังกล่าวจัดว่า 'รุนแรง' โดยเฉลี่ยแล้ว ผลกระทบของเหตุการณ์เหล่านี้แพร่กระจายออกไปในวงกว้าง องค์กรต่างๆ คาดการณ์ว่าค่าใช้จ่ายทางการเงินรวมๆ ของเหตุการณ์ด้านความปลอดภัยข้อมูลที่ร้ายแรงที่สุดอยู่ที่ประมาณ 244,000 ดอลลาร์ ซึ่งหมายความว่าเหตุการณ์ในทุกปีอาจมีค่าใช้จ่ายสูงถึง 15 ล้านดอลลาร์ นอกเหนือจากค่าใช้จ่ายเหล่านี้ ผู้มีอำนาจตัดสินใจ 4 ใน 10 รายยังกล่าวว่าค่าใช้จ่ายในการดำเนินการเพื่อกู้คืนเหตุการณ์ด้านความปลอดภัยข้อมูลและการสูญเสียธุรกิจจากความเสียหายต่อชื่อเสียง เป็นเรื่องที่น่ากังวลอย่างมาก

นอกจากนี้ 92% เผชิญกับความท้าทายหลักๆ ในด้านต้นทุน การบูรณาการ และเวลาในการดำเนินการ ซึ่งขัดขวางความสามารถในการลงทุนในการรักษาความปลอดภัยข้อมูลเพิ่มเติม ตอกย้ำความต้องการโซลูชันที่เหมาะกับงบประมาณและแรงงานที่มีประสิทธิภาพมากขึ้น

การรับรู้ถึงความเชื่อมั่นในความพร้อมด้านความปลอดภัยข้อมู ลแตกต่างจากความเป็นจริงของเหตุการณ์ที่องค์กรกำลังประสบอยู่ แม้ว่าเป็นสิ่งสำคัญสำหรับองค์กรที่จะต้องรู้ว่าข้อมูลอยู่ที่ไหนและตรวจจับความเสี่ยง แต่มาตรการเหล่านี้แบบทีละรายการหรือแยกกันไม่เพียงพอที่จะช่วยให้องค์กรป้องกันเหตุการณ์เพื่อการรักษาความปลอดภัยข้อมูล และไม่ให้ผู้มีอำนาจตัดสินใจด้านความเสี่ยงต้อนตื่นในเวลากลางคืน

ดังที่ CISO (ประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัยข้อมูล) ในองค์กรบริการทางการเงินกล่าวไว้ “ฉันไม่สามารถบอกคณะกรรมการบริหารของฉันได้ว่า 'ฉันรักษาความปลอดภัยข้อมูล แต่ฉันแค่ไม่ได้ปกป้องมัน'... สิ่งสุดท้ายที่เราอยากเห็นก็คือ ธนาคารล่มบนหน้าแรกของ Wall Street Journal”

59

จำนวนเหตุการณ์ด้านความปลอดภัยข้อมูลโดยเฉลี่ยในช่วง 12 เดือนที่ผ่านมา

สูงสุดถึง

$15 ล้าน

ค่าใช้จ่ายต่อปีของเหตุการณ์ความปลอดภัยที่รุนแรง

2

การมีเครื่องมือมากขึ้นไม่ได้หมายความว่ามีความปลอดภัยหรือประสิทธิภาพของข้อมูลมากขึ้น แต่เป็นสิ่งที่ตรงกันข้าม

การมีเครื่องมือมากขึ้นไม่ได้หมายความว่ามีความปลอดภัยหรือประสิทธิภาพของข้อมูลมากขึ้น แต่เป็นสิ่งที่ตรงกันข้าม

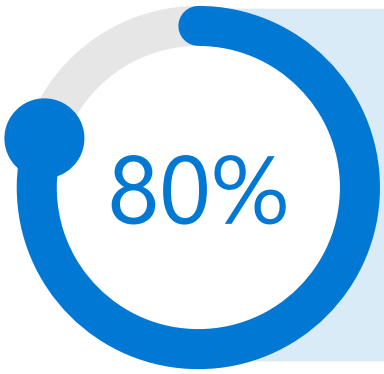
องค์กรต่างๆ เริ่มตระหนักว่าโซลูชันเฉพาะจุดที่ใช้มาเป็นเวลาหลายปี ได้สร้างช่องว่างในการมองเห็นและประสิทธิภาพ เนื่องจากเครื่องมือรักษาความปลอดภัยข้อมูลเป็นแบบแยกส่วน แนวโน้มดังกล่าวกำลังเปิดทางให้กับความปรารถนาที่จะมีโซลูชันแบบครบวงจรสำหรับการรักษาความปลอดภัยข้อมูล โดย 80% ยอมรับว่าแพลตฟอร์มการรักษาความปลอดภัยข้อมูลแบบครบวงจรพร้อมโซลูชันแบบผสานรวมนั้นเหนือกว่าการใช้โซลูชันที่ดีสุดที่ต้องบูรณาการและจัดการด้วยตนเอง

แม้ว่าคนส่วนใหญ่จะถือว่าโซลูชันแบบผสานรวมเหนือกว่า แต่การใช้เครื่องมือรักษาความปลอดภัยข้อมูลก็มีมากมายและกระจัดกระจาย

ด้วยเหตุนี้ องค์กรต่างๆ จึงรายงานว่าใช้เครื่องมือรักษาความปลอดภัยข้อมูลโดยเฉลี่ย 10 รายการเพื่อจัดการกับความเสี่ยงด้านความปลอดภัยข้อมูล รวมถึงการป้องกันข้อมูลสูญหาย, การปกป้องข้อมูล, การจัดการความเสี่ยงจากภายใน, การจัดการข้อมูลด้านความปลอดภัยและเหตุการณ์ (SIEM), Cloud Access Security Broker และอื่นๆ อีกมากมาย สำหรับองค์กรที่มีพนักงานมากกว่า 5,000 คน จำนวนเครื่องมือโดยเฉลี่ยก็จะเพิ่มมากขึ้น

การมีเครื่องมือมากขึ้นอาจสร้างความรู้สึกผิดๆ เกี่ยวกับความปลอดภัย เนื่องจากผู้ที่ใช้เครื่องมือมากกว่า (16 รายการขึ้นไป) มีความมั่นใจในมาตรการรักษาความปลอดภัยข้อมูลของตนมากกว่า เมื่อเทียบกับผู้ที่ใช้เครื่องมือน้อยกว่า (61% เทียบกับ 56%)

อย่างไรก็ตาม การวิจัยขัดแย้งกับความรู้สึกด้านความปลอดภัย เนื่องจากองค์กรที่มีเครื่องมือ 16 รายการ หรือมากกว่า ก็ประสบปัญหาด้านความปลอดภัยข้อมูลมากขึ้นเช่นกัน ในปีที่ผ่านมา โดยเฉลี่ย 133 เหตุการณ์ เทียบกับ 48 เหตุการณ์สำหรับองค์กรที่มีเครื่องมือน้อยกว่า

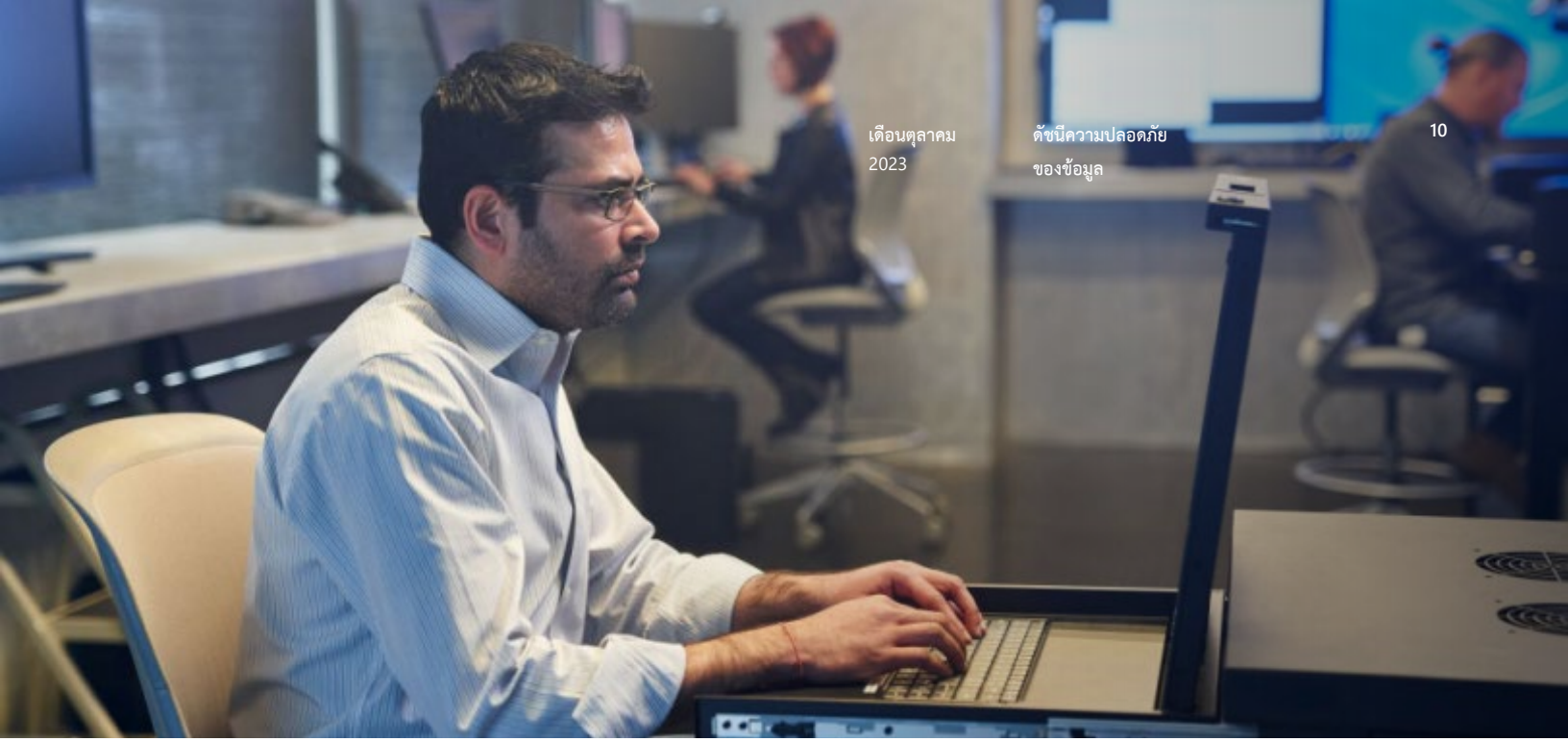


ยอมรับว่าแพลตฟอร์มความปลอดภัยที่ครอบคลุมพร้อมโซลูชันแบบครบวงจรนั้นเหนือกว่าการใช้โซลูชันที่ดีที่สุดหลายตัวที่ต้องมีการผสานรวมและจัดการด้วยตนเอง

2.8 เท่า

เหตุการณ์ด้านความปลอดภัยข้อมูลเพิ่มมากขึ้นในปีที่ผ่านมา

สำหรับองค์กรที่มีเครื่องมือ 16 รายการขึ้นไป (เทียบกับองค์กรที่มีเครื่องมือน้อยกว่า)



กรณีของการรักษาความปลอดภัยข้อมูลที่ดีขึ้นผ่านโซลูชันที่บูรณาการมากขึ้นและเครื่องมือที่น้อยลง จะยิ่งแข็งแกร่งขึ้นเมื่อพิจารณาจากความรู้สึกและแนวทางปฏิบัติของผู้ที่ต้องการโซลูชันที่ดีที่สุดหรือเครื่องมือที่มากขึ้น

“ข้อมูลจะถูกสะสม รวบรวม และใช้จากระบบไม่กี่ระบบอย่างไร จำเป็นต้องรวบรวมจุดข้อมูลที่แตกต่างกันจำนวนมากไว้ในระบบนิเวศเดียวเพื่อให้ใช้งานได้จริง หรือมิฉะนั้น คุณมีความปลอดภัยข้อมูลเวอร์ชัน Swiss cheese จริงๆ”

รองประธานฝ่ายไอที
การผลิต/โปรดักชัน

ประการแรก เครื่องมือรักษาความปลอดภัยข้อมูลที่แตกต่างกันหลายตัวอาจทำให้เกิดช่องว่างในการมองเห็นและข้อมูลเงาที่มากขึ้น ในความเป็นจริง ผู้ที่มีความกังวลเกี่ยวกับข้อมูลเงามักจะชอบโซลูชันที่ดีที่สุด ซึ่งมีแนวโน้มมากกว่า เพราะองค์กรที่มีแนวทางที่ดีที่สุดจำเป็นต้องใช้ความพยายามมากขึ้นเพื่อให้มองเห็นสถานะความปลอดภัยข้อมูลได้อย่างครอบคลุม

ประการที่สอง การจัดการโซลูชันแบบแยกส่วนทำให้ทีมรักษาความปลอดภัยข้อมูลมีความซับซ้อนมากขึ้น เนื่องจากแต่ละโซลูชันที่แตกต่างกันต้องใช้พนักงานเฉพาะด้าน การติดตั้งและบำรุงรักษาเอเจนต์ปลายทาง และกระบวนการใหม่ต่างๆ ยกตัวอย่างการตรวจสอบและคัดแยกการแจ้งเตือน ซึ่งเป็นหนึ่งในงานที่ต้องใช้พนักงานและทรัพยากร จำนวนการแจ้งเตือนที่เพิ่มขึ้นหมายถึงความพยายามเพิ่มเติมของทีมรักษาความปลอดภัยข้อมูลในการจัดการโซลูชันแบบแยกส่วน องค์กรที่มีเครื่องมือมากกว่าจะได้รับการแจ้งเตือนความปลอดภัยข้อมูลโดยเฉลี่ย 96 รายการต่อวัน ในขณะที่ทีมที่มีเครื่องมือน้อยกว่าจะได้รับการแจ้งเตือนน้อยกว่าครึ่งหนึ่ง โดยอยู่ที่ 44 รายการ นอกจากนี้ พวกเขายังไม่สามารถตรวจสอบการแจ้งเตือนเหล่านี้ได้มากเท่ากับทีมที่มีเครื่องมือน้อยกว่า (61% เทียบกับ 68%) ซึ่งมักส่งผลให้องค์กรที่มีเครื่องมือมากกว่า เป็นเชิงรับมากกว่าเมื่อเปรียบเทียบกับองค์กรที่ใช้เครื่องมือในปริมาณน้อยกว่า

สุดท้ายนี้ มีเครื่องมือเพิ่มเติมบ่งชี้ว่าองค์กรต่างๆ ต้องใช้ความพยายามในวงกว้างเพื่อการบูรณาการข้อมูลเชิงลึกและแผนการแก้ไข และข้อมูลอาจสูญหายไปในการแปลเมื่อถามเกี่ยวกับความท้าทายด้านความปลอดภัยข้อมูลอันดับต้นๆ ค่าใช้จ่ายในการปรับใช้หรือบำรุงรักษาโซลูชันความปลอดภัยข้อมูล และความท้าทายในการบูรณาการโซลูชันความปลอดภัยข้อมูลได้รับการจัดอันดับให้เป็นสองอันดับแรก

ส่งผลให้กระบวนการใช้เวลานานและช้าลง โดย 37% ของผู้ใช้เครื่องมือ 16 รายการขึ้นไปรายงานว่าต้องใช้เวลา 1 เดือนหรือนานกว่านั้นในการตรวจสอบความปลอดภัยข้อมูลให้เสร็จสิ้น เทียบกับเพียง 21% ของผู้ที่ใช้เครื่องมือน้อยกว่า

“ตอนนี้เรากำลังเดินหน้าอย่างช้าๆ ทุกระบบที่เรามีล้วนแต่มีพอร์ทัลของตัวเอง เครื่องมือของตัวเอง มีวิธีจัดการกับสิ่งต่างๆ ในแบบของตัวเอง แต่ละคนไปตามทางที่ตัวเองเชี่ยวชาญ จากนั้นพวกเขาทั้งหมดจะกลับมารวมกันและตัดสินใจว่าเกิดอะไรขึ้น และเราจะจัดการจากตรงนั้น ในตอนนี้ มันเป็นการทำงานแบบแมนวลเล็กน้อย” ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานและการปฏิบัติการด้านการผลิตและโปรดักชันกล่าว

ท้ายที่สุดแล้ว องค์กรต่างๆ เลือกที่จะดำเนินการต่อโดยใช้โซลูชันต่างๆ มากมาย โดยไม่สนใจคำพูดของตนเองเกี่ยวกับความเข้าใจที่ว่าโซลูชันแบบผสานรวมนั้นเหนือกว่า และเดินไปในทิศทางตรงกันข้าม ซึ่งส่งผลให้ต้องเสียเวลาและค่าใช้จ่าย

ผลลัพธ์ของผู้ที่ใช้เครื่องมือรักษาความปลอดภัยข้อมูลน้อยกว่า (<16) เทียบกับมากกว่า (16+)	เครื่องมือปริมาณน้อย	เครื่องมือปริมาณมาก
จำนวน**เหตุการณ์ด้านความปลอดภัยข้อมูล**ในช่วง 12 เดือนที่ผ่านมา	**48**	**133**
สัดส่วนของเหตุการณ์ด้านความปลอดภัยข้อมูล**ที่รุนแรง**	**19%**	**26%**
กลยุทธ์การรักษาความปลอดภัยข้อมูลในปัจจุบันของเราเป็น**เชิงรับ**มากกว่า	**31%**	**40%**
ท้าทายด้วยโซลูชันโซลูชัน**การผสานรวม**	**24%**	**39%**
ทีมรักษาความปลอดภัยข้อมูลใช้เวลาส่วนใหญ่กับ**การตอบสนอง**	**19%**	**26%**
เรามี**ความมั่นใจ**กับมาตรการรักษาความปลอดภัยข้อมูลของเรา	**56%**	**61%**
จำนวนการแจ้งเตือนที่**ได้รับ**ต่อวันโดยเฉลี่ย	**การแจ้งเตือนมัลแวร์ 44**	**การแจ้งเตือนมัลแวร์ 96**
สัดส่วนของการแจ้งเตือนที่เราสามารถ**ตรวจสอบ**ได้ต่อวัน	**68%**	**61%**
ต้องใช้เวลา 1 เดือนหรือนานกว่านั้น เพื่อทำการตรวจสอบความปลอดภัยข้อมูลให้เสร็จสิ้น	**21%**	**37%**

3

องค์กรต่างๆ ยังคงต้องเผชิญกับความเครียดจากเหตุการณ์ด้านความปลอดภัยข้อมูลทั้งภายนอกและภายใน โดยเฉพาะอย่างยิ่งข้อมูลทางธุรกิจ

องค์กรต่างๆ ยังคงต้องเผชิญกับความเครียดจากเหตุการณ์ด้านความปลอดภัยข้อมูลทั้งภายนอกและภายใน โดยเฉพาะอย่างยิ่งกับข้อมูลทางธุรกิจ

เนื่องจากปัจจัยเกี่ยวกับข้อมูล รวมถึงบุคคลที่โต้ตอบกับข้อมูล กิจกรรมเกี่ยวกับข้อมูล ตลอดจนอุปกรณ์และแอปที่ใช้ในการประมวลผลข้อมูลมีการเปลี่ยนแปลงอยู่ตลอดเวลา เหตุการณ์ด้านความปลอดภัยข้อมูลและการละเมิดข้อมูลจึงสามารถเกิดขึ้นได้ทุกที่ทุกเวลา และภัยคุกคามเหล่านี้มาจากทั้งผู้โจมตีภายนอกและบุคลากรที่เชื่อถือได้ รวมถึงพนักงาน ผู้รับเหมา และคู่ค้า ไม่ว่าจะโดยเจตนาร้ายหรือโดยไม่ได้ตั้งใจ ผู้เล่นทุกคนสามารถก่อให้เกิดเหตุการณ์ด้านความปลอดภัยข้อมูลได้ ซึ่งหมายความว่ามีความจำเป็นในการปกป้องในหลายพื้นที่อย่างต่อเนื่อง

รองประธานฝ่ายไอทีของบริษัทบริการทางการเงินกล่าว “สิ่งที่คุณพยายามป้องกันนั้นเปลี่ยนแปลงอยู่เสมอ มันเป็นเป้าหมายที่เคลื่อนไหว จะพัฒนา เปลี่ยนแปลง และยืดหยุ่นอยู่เสมอ สิ่งที่คุณกำลังปกป้องและทบริเวณนั้นจะมีความหลากหลายมากขึ้นเท่านั้น”

แม้ว่าเหตุการณ์ด้านความปลอดภัยข้อมูลอาจมาจากแหล่งที่มาต่างๆ มากมาย แต่ภัยคุกคามภายนอกของเหตุการณ์เกี่ยวกับมัลแวร์หรือแรนซัมแวร์ ซึ่งเป็นกรณีที่ซอฟต์แวร์ที่เป็นอันตรายแทรกซึมเข้าไปในระบบ ทำให้ผู้โจมตีเข้าถึงระบบหรือเครือข่ายโดยไม่ได้รับอนุญาต นั้นเป็นเหตุการณ์ที่พบบ่อยที่สุด โดย 50% ขององค์กรที่สำรวจกล่าวว่ามีประสบการณ์อย่างน้อย 1 ครั้งในปีที่ผ่านมา

นอกจากนี้ การโจมตีเหล่านี้เป็นจุดที่องค์กรต่างๆ รู้สึกว่ามีความเสี่ยงมากที่สุด โดย 41% กล่าวว่าพวกเขารู้สึกว่ามีเตรียมพร้อมน้อยที่สุดที่จะรับมือกับการโจมตีของมัลแวร์หรือแรนซัมแวร์ในอนาคตปีถัดไป ความรู้สึกถึงช่องโหว่นี้ยิ่งสูงขึ้นไปอีกในกลุ่มที่ต้องการแนวทางที่ดีที่สุด โดย 44% รู้สึกไม่พร้อมสำหรับการโจมตีในลักษณะนี้เทียบกับเพียง 36% ของผู้ที่ต้องการโซลูชันแบบผสานรวม

การรักษาความปลอดภัยและป้องกันความเสี่ยงจากภายในเป็นสิ่งสำคัญสำหรับผู้มีอำนาจตัดสินใจ 35% กล่าวว่าพวกเขาจำเป็นต้องเสริมการป้องกันบุคคลภายในที่เป็นอันตรายและบัญชีที่ถูกบุกรุก และ 1 ใน 3 เกี่ยวข้องกับเหตุการณ์จากภายในโดยไม่ได้ตั้งใจ แม้ว่าเหตุการณ์ภายในที่เป็นอันตรายอาจไม่ได้เป็นสาเหตุหลักของการละเมิดความปลอดภัยข้อมูล แต่ก็เป็นประเภทเหตุการณ์ที่เกิดขึ้นบ่อยเป็นอันดับสอง ซึ่งผู้มีอำนาจตัดสินใจรู้สึกว่ามีความพร้อมในการป้องกันน้อยที่สุด

“ฉันได้รับโทรศัพท์จากผู้อำนวยการที่ตื่นตระหนก อย่างน้อยเดือนละครั้ง... “เรามีเหตุการณ์ ฉันค้นพบเหตุการณ์ หรือทีมภัยคุกคามได้ค้นพบเหตุการณ์” บางคนไม่ได้ตั้งใจ บางคนไม่รู้หรือเข้าใจว่าสิทธิพิเศษของพวกเขาอนุญาตอะไรบ้าง”

CISO ของรัฐบาลสหรัฐอเมริกา

คนวงในคือบุคคลที่เชื่อถือได้ ซึ่งโดยปกติแล้วจะได้รับอนุญาตให้เข้าถึงหรือมีความรู้เกี่ยวกับทรัพยากร ข้อมูล หรือระบบของบริษัท ซึ่งโดยทั่วไปไม่เปิดเผยต่อสาธารณะ ด้วยเหตุนี้ ความเสี่ยงด้านความปลอดภัยข้อมูลที่เกี่ยวข้องกับบุคคลภายในจึงมีแนวโน้มที่ยากจะเข้าใจและตรวจพบได้ยาก ดังที่ Bret Arsenault ซึ่งเป็น CISO ของ Microsoft ระบุว่า “ท้ายที่สุดแล้ว ไม่สำคัญว่าการละเมิดนั้นจะเกิดขึ้นโดยตั้งใจหรือโดยไม่ได้ตั้งใจ โปรแกรมความเสี่ยงจากภายในควรเป็นส่วนหนึ่งของกลยุทธ์ด้านความปลอดภัยของทุกบริษัท”

สรุปเหตุการณ์ด้านความปลอดภัยข้อมูล

สาเหตุของเหตุการณ์ด้านความปลอดภัยข้อมูล	เหตุการณ์ที่พบบ่อยที่สุดในช่วง 12 เดือนที่ผ่านมา	เตรียมป้องกันน้อยที่สุดในช่วง 12 เดือนข้างหน้า
มัลแวร์หรือแรนซัมแวร์	**50%**	**41%**
บัญชีที่โดนบุกรุก	**38%**	**35%**
การโจมตีการปฏิเสธการให้บริการ (DoS)	**35%**	**33%**
บุคคลภายในที่ละเลย	**32%**	**29%**
บุคคลภายในที่ไม่ตั้งใจ	**31%**	**32%**
บุคคลภายในที่เป็นอันตราย	**31%**	**35%**
คุณสมบัติทางกายภาพ	**29%**	**29%**

โซลูชันการรักษาความปลอดภัยข้อมูลที่องค์กรเลือกจะต้องใช้ได้กับข้อมูลที่ละเอียดอ่อนหลายประเภท รวมถึงข้อมูลธุรกิจที่มีมูลค่าสูง ข้อมูลการดำเนินงาน และข้อมูลส่วนบุคคล ในช่วงเหตุการณ์ด้านความปลอดภัยข้อมูล 12 เดือนที่ผ่านมา 74% ขององค์กรถูกเปิดเผยข้อมูลทางธุรกิจ, 65% เห็นว่าข้อมูลการปฏิบัติงานถูกบุกรุก และ 58% ประสบปัญหาข้อมูลส่วนบุคคลตกอยู่ในความเสี่ยง ในบรรดาข้อมูลประเภทต่างๆ ทรัพย์สินทางปัญญา การออกแบบไอทีและเครือข่าย และ PII ถูกบุกรุกหรือเปิดเผยบ่อยที่สุด

เมื่อมองไปข้างหน้า 77% ขององค์กรมองว่าข้อมูลทางธุรกิจ เช่น ทรัพย์สินทางปัญญาและซอร์สโค้ดเป็นกลุ่มที่มีช่องโหว่มากที่สุด สาเหตุหลักมาจากข้อมูลทางธุรกิจมีบทบาทสำคัญในการสร้างความได้เปรียบทางการแข่งขันและการสร้างรายได้ อย่างไรก็ตาม การระบุและจำแนกข้อมูลดังกล่าวอาจเป็นเรื่องที่ท้าทาย เนื่องจากการจดจำรูปแบบแบบดั้งเดิม การแสดงออกตามปกติหรือเทคโนโลยีการจับคู่ฟังก์ชัน อาจไม่สามารถระบุเนื้อหาที่ขาดรูปแบบสตริงหรือคำหลักที่เฉพาะเจาะจงได้อย่างมีประสิทธิภาพ ในทางกลับกัน องค์กรต่างๆ ต้องการเทคโนโลยีขั้นสูงเพิ่มเติมเพื่อช่วยค้นหาและปกป้องข้อมูลที่ละเอียดอ่อนที่มีช่องโหว่เหล่านั้น

ประเภทของข้อมูลที่มีความเสี่ยงมากที่สุดในอีก 12 เดือนข้างหน้า

77% ข้อมูลทางธุรกิจ		64% ข้อมูลการดำเนินงาน		63% ข้อมูลส่วนบุคคล	
ทรัพย์สินทางปัญญา	30%	การออกแบบไอทีและเครือข่าย	29%	ข้อมูลส่วนบุคคลและข้อมูลที่สามารถระบุตัวตนได้ (PII)	31%
ซอร์สโค้ด	28%	งบการเงิน	18%	ข้อมูลทรัพยากรบุคคล (เงินเดือน ประวัติย่อ ฯลฯ)	21%
แผนธุรกิจ	27%	รายงานยอดขายและรายได้	15%	ข้อมูลอุตสาหกรรมบัตรชำระเงิน (PCI)	18%
ความลับทางการค้า	24%	การจัดซื้อและใบแจ้งหนี้	12%	ข้อมูลด้านสุขภาพที่ได้รับการคุ้มครอง (PHI)	18%
ไฟล์การควบรวมกิจการ	20%	เอกสาร/ข้อตกลงทางกฎหมาย	12%	ข้อมูลประจำตัว	17%
ข้อมูลจำเพาะเกี่ยวกับการก่อสร้าง	18%	กระบวนการผลิต/แบตช์ไฟล์	11%		

4

องค์กรต่างๆ ต้องการระบบคลาวด์และ AI เพื่อขับเคลื่อนการเปลี่ยนแปลงทางดิจิทัล แต่ก็เป็นจุดที่ข้อมูลที่มีความเสี่ยงมากที่สุดเช่นกัน

องค์กรต่างๆ ต้องการระบบคลาวด์และ AI เพื่อขับเคลื่อนการเปลี่ยนแปลงทางดิจิทัล แต่ก็เป็นจุดที่ข้อมูลที่มีความเสี่ยงมากที่สุดเช่นกัน

การทำงานร่วมกันผ่านแอปพลิเคชันและแพลตฟอร์มบนคลาวด์รวมกับเทคโนโลยี AI ใหม่ๆ ช่วยเพิ่มประสิทธิภาพการทำงานของพนักงานได้อย่างมาก และช่วยให้สามารถจัดเตรียมการทำงานที่ยืดหยุ่น ทำให้แอปพลิเคชันบนคลาวด์และเทคโนโลยี AI จำเป็นสำหรับองค์กร โดยเฉลี่ยแล้วปัจจุบันองค์กรต่างๆ ใช้บริการคลาวด์สาธารณะ 147 บริการ ครอบคลุมถึง SaaS, PaaS, และ IaaS[1] และ 66% ขององค์กรได้พัฒนากลยุทธ์ AI โดย 36% ได้นำไปปรับใช้แล้ว[2] อย่างไรก็ตาม วิวัฒนาการนี้ได้สร้างความเสี่ยงแบบไดนามิกและหลายแง่มุมมากขึ้น เนื่องจากความยากลำบากในการกำหนดขอบเขตข้อมูลอย่างชัดเจนในสภาพแวดล้อมต่างๆ

ตอนนี้การมีโซลูชันการรักษาความปลอดภัยข้อมูลที่เหมาะสมสำหรับตำแหน่งข้อมูลที่มีประสิทธิผลสูงเหล่านี้มีความสำคัญมากยิ่งขึ้น ในช่วง 12 เดือนที่ผ่านมา 42% ขององค์กรรายงานเหตุการณ์ด้านความปลอดภัยในพื้นที่เก็บข้อมูลบนคลาวด์ และ 31% รายงานในอีเมล ข้อความโต้ตอบ หรือเครื่องมือการประชุมออนไลน์ เหตุการณ์ต่างๆ ดูเหมือนจะเกิดขึ้นบ่อยที่สุดในส่วนที่เกิดประสิทธิภาพการทำงานและการทำงานร่วมกันมากที่สุด

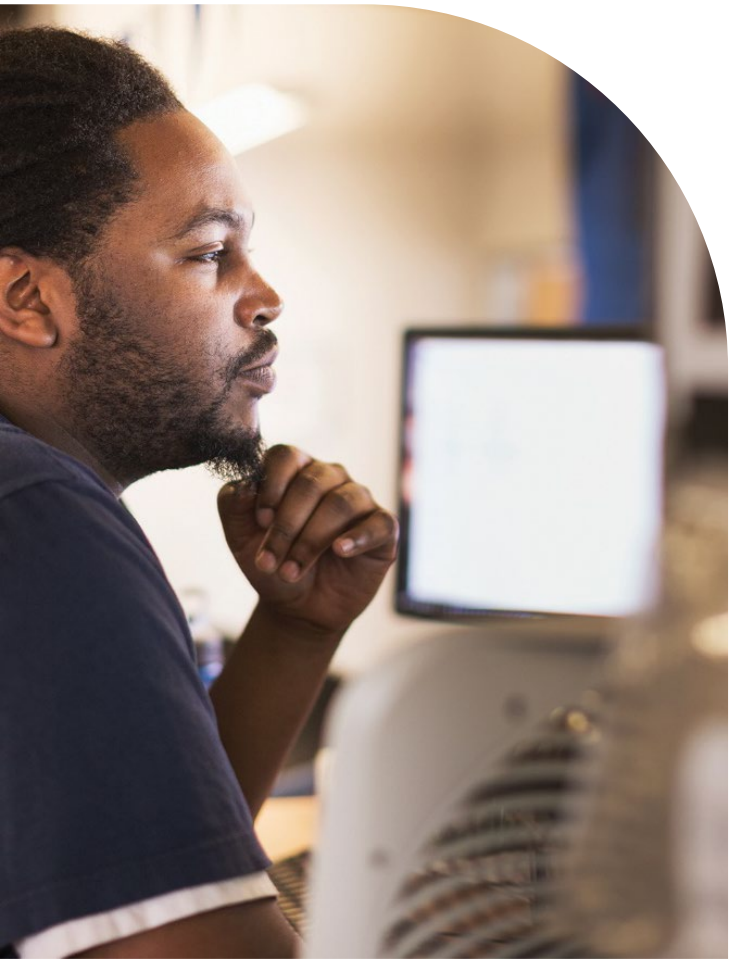
การจัดการเหตุการณ์ประเภทนี้ต้องใช้ทรัพยากร และ 79% ขององค์กรรายงานว่าทีมรักษาความปลอดภัยข้อมูลของพวกเขาต้องการบุคลากรมากขึ้นเพื่อจัดการความรับผิดชอบด้านความปลอดภัยข้อมูลที่สำคัญอย่างมีประสิทธิภาพ อย่างไรก็ตาม ในบรรดาองค์กรต่างๆ ที่อ้างว่าต้องการคนมากขึ้น ส่วนใหญ่ (57%) ชอบแนวทางเครื่องมือที่ดีที่สุด การกำหนดค่านี้เน้นย้ำว่าองค์กรที่ใช้โซลูชันมากขึ้นอาจต้องดิ้นรนมากขึ้นเพื่อระบุความเสี่ยงที่แท้จริงในกิจกรรมของผู้ใช้จำนวนมากมาย

1. Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022
2. การวิจัย AI การรักษาความปลอดภัยข้อมูลของ Microsoft, Hypothesis, มี.ค. 2023

สรุปตำแหน่งข้อมูล

ตำแหน่งข้อมูล	ถูกบุกรุกในช่วง 12 เดือนที่ผ่านมา	มีความเสี่ยงมากที่สุด
ที่เก็บข้อมูลบนคลาวด์ (เช่น Box, OneDrive, Google Drive)	42%	54%
อีเมล/ข้อความโต้ตอบ/เครื่องมือการประชุมออนไลน์	31%	39%
ระบบการให้บริการแพลตฟอร์มด้านไอที (PaaS)	29%	34%
การให้บริการโครงสร้างพื้นฐานด้านไอที (IaaS)	28%	36%
AI (เช่น ChatGPT, Bard ฯลฯ)	27%	38%
ฐานข้อมูล/Data Lake ที่ใช้ SaaS	27%	41%
อุปกรณ์ปลายทาง/อุปกรณ์	25%	36%
ที่เก็บข้อมูลภายในองค์กร/การแชร์ไฟล์/ฐานข้อมูล	24%	28%
ข้อมูลเงา	21%	23%
แอปพลิเคชันสายงานธุรกิจ	17%	25%
เครื่องมือสำหรับนักพัฒนา	16%	23%

ด้วยองค์กรมากกว่า 1 ใน 3 กำลังปรับใช้กลยุทธ์ AI และอีกหลายแห่งที่กำลังดำเนินการ ซึ่ง AI กำลังถูกนำไปใช้ในอัตราที่ไม่เคยมีมาก่อน ซึ่งเร็วกว่าการนำระบบคลาวด์และอีเมลมาใช้ในอดีตมาก ในขณะที่องค์กรต่างๆ หันมาใช้ AI ทำให้การยกระดับความปลอดภัยข้อมูลเพื่อให้สามารถใช้งานได้อย่างมีความรับผิดชอบและป้องกันความเสี่ยงจึงกลายเป็นสิ่งจำเป็น AI ถือเป็นจุดที่มีความเสี่ยงอันดับต้นๆ สำหรับเหตุการณ์ด้านความปลอดภัยข้อมูล เมื่อเปรียบเทียบกับส่วนอื่นๆ และ 27% ขององค์กรประสบปัญหาการละเมิดความปลอดภัยข้อมูล AI ความกังวลขององค์กรเกี่ยวกับความเสี่ยงในการใช้ศูนย์ AI ที่การขาดการควบคุมข้อมูลที่แชร์กับ AI, การขาดการควบคุมในการตรวจจับและบรรเทาการใช้งาน AI ที่มีความเสี่ยง, การขาดความโปร่งใสเกี่ยวกับวิธีการฝึกอบรมโมเดล AI เชิงสร้างสรรค์ และการรั่วไหลของข้อมูลที่เป็นความลับผ่าน AI



“AI นั้นดีต่อประสิทธิภาพและประสิทธิผล แต่อาจมีความเสี่ยงด้านความปลอดภัยและข้อมูล” ผู้มีอำนาจตัดสินใจด้านความปลอดภัยในองค์กรระบุไว้

แม้ว่าข้อกังวลเกี่ยวกับ AI ยังคงมีอยู่ ผู้มีอำนาจตัดสินใจก็มองเห็นศักยภาพเช่นกัน โดยเฉพาะอย่างยิ่งเมื่อผู้ขายในตลาดกำลังพัฒนานวัตกรรมเพื่อช่วยธุรกิจต่างๆ ผ่านการใช้ AI ที่มีความรับผิดชอบ อย่างไรก็ตาม เพื่อใช้ประโยชน์จาก AI ต่อไป องค์กรต่างๆ รายงานการควบคุมระดับสูงที่พวกเขาต้องการ ได้แก่ การตรวจจับเนื้อหาที่เป็นอันตรายหรือมีความเสี่ยงใน AI, เข้ารหัส, ปิดบัง หรือทำให้ข้อมูลเป็นนิรนามก่อนที่จะอัปโหลดไปยัง AI และระบุข้อมูลที่ละเอียดอ่อนที่สร้างโดย AI

การควบคุมความปลอดภัยข้อมูล 5 อันดับแรกที่จำเป็นสำหรับ AI

1	**ตรวจจับเนื้อหาที่เป็นอันตรายหรือมีความเสี่ยงใน AI**
2	**เข้ารหัส ปิดบัง หรือทำให้ข้อมูลเป็นนิรนาม ก่อนที่จะอัปโหลดไปยัง AI**
3	**ระบุข้อมูลที่ละเอียดอ่อนที่สร้างโดย AI**
4	**ป้องกันข้อมูลที่ละเอียดอ่อนจากการอัปโหลดไปยัง AI**
5	**ตรวจจับโมเดลหรือการจัดการข้อมูลใน AI**

5

ระบบอัตโนมัติและ AI จึงเป็นแนวทางในการปกป้องที่ดียิ่งขึ้น

ระบบอัตโนมัติและ AI จึงเป็นแนวทางในการปกป้องที่ดียิ่งขึ้น

ในโลกอุดมคติ องค์กรครึ่งหนึ่งต้องการดำเนินการเชิงรุกเกี่ยวกับการจัดการความปลอดภัยข้อมูลมากขึ้น โดยปราศจากข้อจำกัดตามลำดับความสำคัญหรืองบประมาณขององค์กร ใช้เวลามากขึ้นกับสิ่งต่างๆ เช่น การค้นพบข้อมูลที่ละเอียดอ่อนและความเสี่ยงที่เกี่ยวข้อง และการป้องกันเหตุการณ์ด้านความปลอดภัยข้อมูล แม้ว่าในปัจจุบัน องค์กรมากกว่าครึ่งหนึ่งใช้เวลาส่วนใหญ่มุ่งเน้นไปที่มาตรการเชิงรับ เช่น การตรวจจับเหตุการณ์ การตอบสนอง และการตรวจสอบ และการตรวจจับและการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของข้อมูลนี้ต้องใช้เวลามาก โดยองค์กรส่วนใหญ่ใช้เวลาประมาณหนึ่งเดือนในการแก้ไขเหตุการณ์ด้านความปลอดภัยข้อมูล และสำหรับบางบริษัท การแก้ปัญหาอาจใช้เวลานานถึง 6 เดือน

ประโยชน์ของการใช้กลยุทธ์เชิงรุกมากขึ้นนั้นมองเห็นได้ชัดเจน เนื่องจากองค์กรที่สำรวจเชิงรุกมากขึ้นนั้นประสบกับเหตุการณ์ด้านความปลอดภัยข้อมูลที่มีค่าใช้จ่ายน้อยกว่า มีแนวโน้มที่จะสามารถตรวจสอบเหตุการณ์เหล่านั้นได้ในเวลาน้อยกว่า 1 เดือน และมีแนวโน้มที่จะเชื่อได้ว่าการควบคุมการป้องกันนั้นเพียงพอในการป้องกันการละเมิดข้อมูลได้มากขึ้น

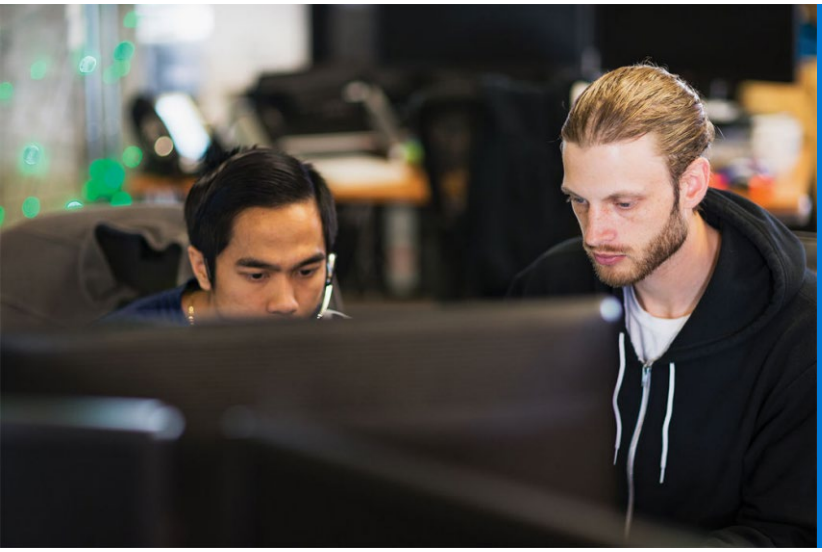
แม้ว่าองค์กรต่างๆ ตระหนักดีว่ามาตรการรักษาความปลอดภัยข้อมูลเชิงรุกสามารถช่วยลดความเสี่ยงด้านความปลอดภัยข้อมูลได้ แต่พวกเขาก็ยังไม่มีความคืบหน้าในการนำมาตรการเหล่านั้นไปใช้ ตัวอย่างเช่น ผู้ที่ต้องการดำเนินการเชิงรุกมากขึ้นโดยจัดสรรเวลาให้กับการป้องกันมากขึ้น มีแนวโน้มที่จะเลือกโซลูชันที่ดีที่สุด ซึ่งจริงๆ แล้วต้องการความพยายามมากขึ้นในการจัดการกับมาตรการเชิงรับเมื่อนำสัญญาณการตรวจจับและการควบคุมการตอบสนองมารวมกัน

ผลลัพธ์ขององค์กรที่เป็นเชิงรุกมากกว่าเทียบกับเชิงรับมากกว่า	เชิงรุกมากกว่า	เชิงรับมากกว่า
ผลกระทบด้านต้นทุนโดยเฉลี่ยจากเหตุการณ์ด้านความปลอดภัยข้อมูลในช่วง 12 เดือนที่ผ่านมา	**$207,000**	**$330,000**
ทำการตรวจสอบความปลอดภัยของข้อมูลให้เสร็จสิ้น ในเวลาน้อยกว่า 1 เดือนโดยเฉลี่ย	**80%**	**68%**
การควบคุมการป้องกันของเรานั้นเพียงพอในการป้องกันการละเมิดข้อมูล	**77%**	**68%**

เนื่องจากทรัพยากรและพนักงานมีจำกัดและการจัดสรรความพยายามระหว่างกิจกรรมต่างๆ อาจไม่เหมาะสม องค์กรต่างๆ จึงกำลังมองหาเทคโนโลยีเพื่อช่วยให้พวกเขาจัดสรรเวลาสำหรับกิจกรรมเชิงรุกมากขึ้น ระบบอัตโนมัติเป็นวิธีหนึ่งสำหรับองค์กรในการจัดสรรเวลาสำหรับแนวทางเชิงรุกในการรักษาความปลอดภัยข้อมูล 74% ขององค์กรที่สำรวจต้องการลดความเสี่ยงแบบกึ่งอัตโนมัติหรืออัตโนมัติเต็มรูปแบบ ซึ่งช่วยให้ทีมรักษาความปลอดภัยสามารถลดผลกระทบจากเหตุการณ์ด้านความปลอดภัยข้อมูลที่อาจเกิดขึ้นได้ล่วงหน้า มากกว่าการตรวจสอบแบบแมนวล นอกจากนี้ องค์กรต่างๆ ยังตระหนักถึงงานอื่นๆ อีกมากมายที่อาจได้รับประโยชน์จากระบบอัตโนมัติ เช่น การสร้างรายงานความปลอดภัยข้อมูล เวิร์กโฟลว์การจัดการเหตุการณ์แบบอัตโนมัติ และการตอบสนองต่อและการตรวจสอบเหตุการณ์ งานหลักส่วนใหญ่ที่ทีมรักษาความปลอดภัยต้องการให้ทำให้เป็นระบบอัตโนมัติคือมาตรการเชิงรับ ด้วยการทำให้งานเหล่านี้เป็นอัตโนมัติ องค์กรต่างๆ จึงสามารถแบ่งเบาภาระของทีมรักษาความปลอดภัยข้อมูลได้ ทำให้พวกเขาเปิดรับจุดยืนเชิงรุกมากขึ้น

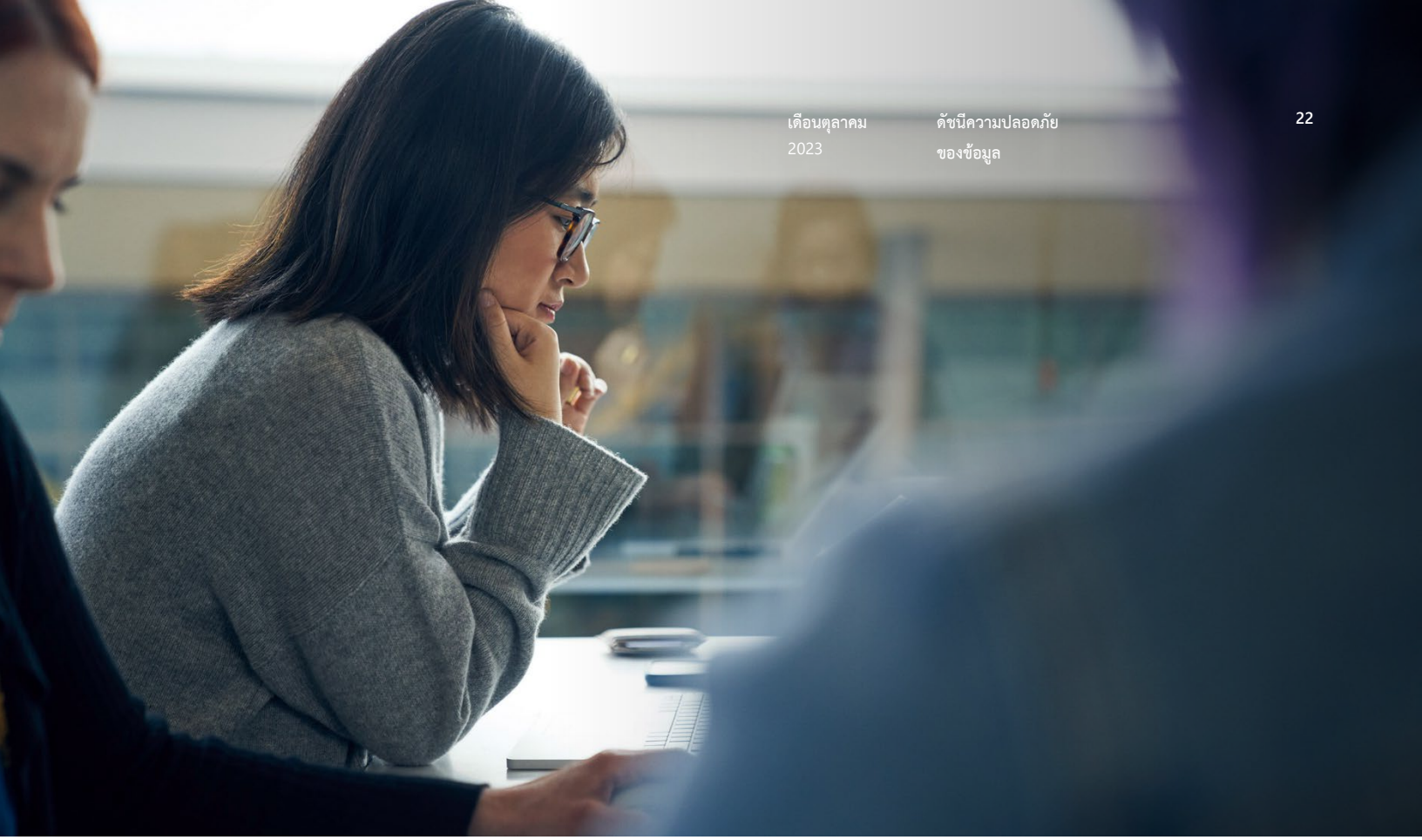
พื้นที่ 5 อันดับแรกที่ทีมรักษาความปลอดภัยข้อมูลอยากให้ดำเนินการอัตโนมัติ/บรรเทา

เชิงรับ	1	การสร้างเวิร์กโฟลว์อัตโนมัติสำหรับการจัดการและการตอบสนองต่อเหตุการณ์
	2	การสร้างรายงานความปลอดภัยข้อมูล
เชิงรับ	3	ตอบสนองและบรรจุเหตุการณ์ด้านความปลอดภัยข้อมูล
	4	การกำหนดเส้นทางเหตุการณ์ไปยังทีมที่เหมาะสม (เช่น SOC, กฎหมาย, HR) ในระหว่างการตรวจสอบ
	5	การตรวจสอบเหตุการณ์ด้านความปลอดภัยข้อมูล



“มีข้อมูลที่มีความเสี่ยงมากมายให้ประเมินด้วยตนเอง AI สามารถช่วยเพิ่มความเร็วในการตอบสนองของทีมเราและปกป้องข้อมูลเนื่องจากเรามีทรัพยากรไม่เพียงพอ”

ผู้มีอำนาจตัดสินใจด้านความปลอดภัยของสหราชอาณาจักร



การใช้ AI เพื่อรักษาความปลอดภัยข้อมูลยังช่วยให้องค์กรมีกลยุทธ์และชาญฉลาดมากขึ้นเกี่ยวกับภัยคุกคามในอนาคต เทคโนโลยีนี้เร่งความเร็วในการตอบสนองต่อเหตุการณ์ที่ตรวจพบ ทำให้ผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลมีเวลาตรวจสอบเพิ่มเติม เช่นเดียวกับระบบอัตโนมัติ องค์กรต่างๆ อ้างถึงหลายสถานการณ์ที่ AI สามารถช่วยรักษาความปลอดภัยให้แข็งแกร่งยิ่งขึ้น **จึงช่วยประหยัดเวลาของทีม** สถานการณ์ยอดนิยมสำหรับการใช้งาน AI ได้แก่ การบล็อกการแชร์ข้อมูลที่ไม่เหมาะสมโดยอัตโนมัติ การตรวจจับความเสี่ยงด้านความปลอดภัยข้อมูลที่สำคัญ/กิจกรรมที่ผิดปกติของข้อมูล และตรวจสอบเหตุการณ์ด้านความปลอดภัยข้อมูลที่อาจเกิดขึ้น

ด้วยการใช้ประโยชน์จาก AI และการสร้างระบบอัตโนมัติและก้าวไปสู่โซลูชันที่ผสานรวมมากขึ้น องค์กรต่างๆ สามารถรับกลยุทธ์การรักษาความปลอดภัยข้อมูลเชิงรุกได้มากขึ้น และเตรียมพร้อมสำหรับอนาคตที่ปลอดภัยยิ่งขึ้น

สถานการณ์ยอดนิยมที่ใช้ AI

การบล็อกการแชร์ข้อมูลที่ไม่เหมาะสม**โดยอัตโนมัติ**

ตรวจจับความเสี่ยงด้านความปลอดภัยของข้อมูลที่สำคัญ/กิจกรรมที่ผิดปกติของข้อมูล

คำแนะนำเพื่อให้สภาพแวดล้อมข้อมูลของคุณปลอดภัยยิ่งขึ้น

ตรวจสอบเหตุการณ์ด้านความปลอดภัยข้อมูลที่อาจเกิดขึ้น

ปรับแต่งนโยบายการรักษาความปลอดภัยข้อมูล

คำแนะนำสุดท้าย

- ใช้แพลตฟอร์มแบบผสานรวมเพื่อเสริมความแข็งแกร่งให้กับมาตรการรักษาความปลอดภัยข้อมูล
- ป้องกันเหตุการณ์ด้านความปลอดภัยข้อมูลทั้งจากภายนอกและภายในด้วยแนวทางการป้องกันเชิงลึก
- อัปเกรดกลยุทธ์การรักษาความปลอดภัยข้อมูลของคุณด้วย AI และระบบอัตโนมัติ

คำแนะนำสุดท้าย

ใช้แพลตฟอร์มแบบผสานรวมเพื่อเสริมความแข็งแกร่งให้กับมาตรการรักษาความปลอดภัยข้อมูล

จากการค้นพบในการวิจัยนี้พบว่าโซลูชันที่น้อยลงสามารถนำมาซึ่งความปลอดภัยได้มากขึ้น อาจดูเหมือนขัดกับสัญชาตญาณ แต่องค์กรต่างๆ จะต้องต่อสู้กับความรู้สึกมั่นใจที่ผิดๆ ที่เกิดขึ้นจากโซลูชันแบบแยกส่วน การรวมผู้จัดจำหน่ายช่วยมอบแนวทางเชิงกลยุทธ์ที่ไม่เพียงแต่ช่วยลดต้นทุน แต่ยังช่วยเพิ่มความปลอดภัยอีกด้วย

ผู้มีอำนาจตัดสินใจด้านความปลอดภัข้อมูลสามารถเริ่มต้นการเปลี่ยนแปลงนี้ได้ด้วยการมอบอำนาจให้ทีมของตนทุ่มเทเวลามากขึ้นในการทำงานเชิงกลยุทธ์ เช่น การค้นคว้าและการวางแผนสำหรับการควบคุมความปลอดภัยใหม่ๆ และการปรับนโยบายความปลอดภัยให้เหมาะสม ซึ่งเป็นสิ่งที่ผู้มีอำนาจตัดสินใจ 84% เห็นด้วยว่าเป็นสิ่งที่พวกเขาต้องการทำ กระบวนการนี้เกี่ยวข้องกับการแทนที่โซลูชันแบบแยกส่วนเดิม ซึ่งมักถูกมองว่าเป็น "ดีที่สุด" แต่ไม่สามารถรวมเข้ากับเครื่องมืออื่นๆ ได้อย่างมีประสิทธิภาพ

ผู้มีอำนาจตัดสินใจสามารถส่งเสริมการทำงานร่วมกันอย่างใกล้ชิดกับทีมของตน เพื่อกำหนดเป้าหมายโปรแกรมความปลอดภัยของข้อมูลและตัวบ่งชี้ประสิทธิภาพหลัก (KPI) จากนั้นพวกเขาสามารถดำเนินการได้โดยการกำหนดข้อกำหนดของโซลูชันและระบุคุณสมบัติที่ไม่สามารถต่อรองได้ แนวทางนี้ช่วยให้พวกเขาสามารถระบุผู้จัดจำหน่ายที่สามารถจัดหาเครื่องมือที่สอดคล้องกับวัตถุประสงค์ที่ครอบคลุมได้ สิ่งสำคัญอย่างยิ่งคือส่งเสริมกรอบความคิดแบบคิดไปข้างหน้า และช่วยให้ทีมหลีกเลี่ยงการยึดติดกับแนวทางปฏิบัติที่มีอยู่หรือกรณีการใช้งานแบบแยกส่วนมากเกินไป ทำให้พวกเขาสามารถนำการเปลี่ยนแปลงที่จำเป็นไปสู่แนวทางที่มีการผสานรวมมากขึ้น

แพลตฟอร์มการรักษาความปลอดภัยของข้อมูลแบบผสานรวมควรช่วยให้ทีมรักษาความปลอดภัยทำงานที่สำคัญเหล่านี้ได้อย่างราบรื่น:

1. ค้นพบและปกป้องข้อมูลที่ละเอียดอ่อนภายในภูมิทัศน์ดิจิทัล
2. ตรวจจับความเสี่ยงที่สำคัญที่เกี่ยวข้องกับข้อมูลนี้
3. ป้องกันการใช้ข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต ในขณะที่ไม่ส่งผลกระทบต่อกิจกรรมทางธุรกิจที่ถูกกฎหมาย

ด้วยการปรับใช้กลยุทธ์การรักษาความปลอดภัยของข้อมูลแบบผสานรวม องค์กรต่างๆ จึงสามารถบรรลุระดับการป้องกันที่สูงขึ้น ในขณะเดียวกันก็ทำให้โครงสร้างพื้นฐานด้านความปลอดภัยง่ายขึ้นไปพร้อมๆ กันได้

คำแนะนำสุดท้าย

ป้องกันเหตุการณ์ด้านความปลอดภัยข้อมูลทั้งจากภายนอกและภายในด้วยแนวทางการป้องกันเชิงลึก

เหตุการณ์ด้านความปลอดภัยข้อมูลมักเกิดจากผู้โจมตีภายนอก บุคคลภายในที่ประสงค์ร้าย หรือบุคคลภายในที่ไม่ได้ตั้งใจ องค์กรต้องใช้มาตรการเพื่อปกป้องข้อมูลของตน ทั้งโดยการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากภัยคุกคามภายนอก และโดยการลดความเสี่ยงของการโจรกรรมข้อมูลภายในหรือการเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ

เพื่อรับมือกับความท้าทายเหล่านี้ องค์กรต่างๆ สามารถใช้แนวทางการป้องกันเชิงลึกในการรักษาความปลอดภัยข้อมูลได้ กลยุทธ์นี้คล้ายคลึงกับการปกป้องงานศิลปะอันล้ำค่าของพิพิธภัณฑ์: กล้องรักษาความปลอดภัยล้ำสมัยที่มาพร้อมกับผู้เยี่ยมชมที่ติดตามข่าวกรองภัยคุกคาม ระบบจองตั๋วจัดการข้อมูลประจำตัวและการเข้าถึงพิพิธภัณฑ์ และมาตรการรักษาความปลอดภัยที่เข้มงวดเกี่ยวกับงานศิลปะทำงานคล้ายกับการควบคุมความปลอดภัยข้อมูลที่ปกป้องข้อมูลที่มีค่าของคุณ มาตรการเหล่านี้ไม่สนับสนุนเหตุการณ์ที่อาจเกิดขึ้น ไม่ว่าจะเกิดจากผู้ไม่ประสงค์ดีภายนอกหรือบุคคลที่อยู่ภายในสภาพแวดล้อมขององค์กร

การต่อสู้กับความเสี่ยงด้านความปลอดภัยข้อมูลที่กำลังพัฒ นาต้องใช้ความพยายามร่วมกันทั่วทั้งองค์กรเพื่อใช้กลยุทธ์การป้องกันเชิงลึกนี้ การทำงานร่วมกันของทีมรักษาความปลอดภัยข้อมูลกับแผนกอื่นๆ เช่น ศูนย์ปฏิบัติการรักษาความปลอดภัย (SOC) สามารถเพิ่มประสิทธิภาพการลงทุนด้านความปลอดภัยข้อมูลได้ โดยเฉพาะอย่างยิ่ง 66% ขององค์กรที่คิดว่าตนเองมีปฏิสัมพันธ์เชิงรุกกับทีม SOC ของตน เทียบกับ 54% ที่ไม่

เช่นเดียวกับการทำงานเป็นทีมในทีมรักษาความปลอดภัย โซลูชันความปลอดภัยข้อมูลควรผสานรวมกับระบบอื่นๆ ได้อย่างราบรื่น เช่น โซลูชันการตรวจจับและการตอบสนองแบบขยาย (XDR) หรือโซลูชันการจัดการข้อมูลประจำตัวและการเข้าถึง (IAM) เพื่อป้องกันเหตุการณ์ด้านความปลอดภัยข้อมูลจากแหล่งข้อมูลทั้งภายนอกและภายในอย่างมีประสิทธิภาพ การผสานรวมเหล่านี้ช่วยให้องค์กรดำเนินการตรวจสอบและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้อย่างครอบคลุม มีความเข้าใจข้อมูล ผู้มีบทบาทและกิจกรรมที่ได้รับผลกระทบอย่างถ่องแท้ และตอบสนองด้วยการควบคุมการลดผลกระทบที่หลากหลายด้วยเหตุนี้ สิ่งนี้จึงช่วยให้พวกเขาสามารถตอบสนองอย่างมีข้อมูล แม่นยำ และรวดเร็ว เพื่อลดผลกระทบจากเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น

คำแนะนำสุดท้าย

อัปเกรดกลยุทธ์การรักษาความปลอดภัยข้อมูลของคุณด้วย AI และระบบอัตโนมัติ

ระบบอัตโนมัติและ AI สามารถช่วยให้องค์กรดำเนินการด้านความปลอดภัยข้อมูลเชิงรุกได้มากขึ้น ต่อไปนี้คือคำแนะนำบางประการสำหรับองค์กรของคุณในการเริ่มใช้ระบบอัตโนมัติและ AI:

- ค้นพบข้อมูลที่ละเอียดอ่อน: ใช้ AI เพื่อช่วยในการระบุข้อมูลที่ละเอียดอ่อนและใช้นโยบายการป้องกัน รวมถึงการเข้ารหัสและการจัดการสิทธิ์ สิ่งนี้มีประโยชน์อย่างยิ่งสำหรับข้อมูลทางธุรกิจที่อาจก่อให้เกิดความท้าทายในการตรวจจับ ผ่านเทคโนโลยีการจดจำรูปแบบดั้งเดิม องค์กรสามารถใช้ประโยชน์จากเทคโนโลยีการจำแนกประเภท เช่น แมชชีนเลิรนนิงหรือตัวแยกประเภทที่ขับเคลื่อนด้วย AI ซึ่งเป็นที่ยอมรับในด้านความฉลาดและความสามารถในการค้นหาเนื้อหาที่ละเอียดอ่อนอย่างรวดเร็ว ตามบริบทของข้อมูลหรือหมวดหมู่ธุรกิจอีกทางหนึ่ง องค์กรต่างๆ สามารถใช้เทคโนโลยีการจับคู่ข้อมูลที่แม่นยำเพื่อค้นพบข้อมูลการปฏิบัติงานหรือข้อมูลส่วนบุคคล

  นอกจากนี้ เมื่อกฎระเบียบทางอุตสาหกรรมมีการเปลี่ยนแปลง (เช่น GDPR, HIPAA, หรือ PCI DSS) และภาพรวมภูมิทัศน์ของข้อมูลมีไดนามิกมากขึ้น จึงจำเป็นอย่างยิ่งที่จะต้องมีเทคโนโลยีการจำแนกประเภทขั้นสูงที่สามารถปรับแต่งและปรับเปลี่ยนได้อย่างง่ายดาย เพื่อระบุหมวดหมู่ใหม่ของข้อมูลที่ละเอียดอ่อน

- ตรวจจับความเสี่ยงด้านความปลอดภัยข้อมูลที่สำคัญ: ควบคุมพลังของ AI เพื่อระบุความเสี่ยงที่สำคัญที่เกี่ยวข้องกับข้อมูลที่ละเอียดอ่อนของคุณ และจัดสรรทรัพยากรอย่างมีกลยุทธ์เพื่อจัดการกับเหตุการณ์ที่มีความเสี่ยงสูงที่อาจเกิดขึ้น เทคโนโลยี AI สามารถสร้างการแจ้งเตือนที่มีความเที่ยงตรงสูง ช่วยให้ทีมรักษาความปลอดภัยประหยัดเวลาอันมีค่าที่อาจจะต้องใช้ในการคัดกรองการแจ้งเตือนที่เป็นบวกเท็จจำนวนมาก นอกจากนี้ AI ยังสามารถช่วยเหลือองค์กรในการระบุความเสี่ยงที่เข้าใจยาก โดยเฉพาะอย่างยิ่งเมื่อผู้ไม่ประสงค์ดีพยายามหลบเลี่ยงการตรวจจับ จำเป็นที่จะต้องใช้ความเร็วของเครื่องเพื่อแซงหน้าผู้คุกคามเหล่านี้

- ป้องกันเหตุการณ์ด้านความปลอดภัยข้อมูลแบบไดนามิก: ใช้ AI และระบบอัตโนมัติเพื่อปรับแต่งการป้องกันและควบคุมการบรรเทาผลกระทบโดยอัตโนมัติตามความเสี่ยงที่ประเมิน สร้างกลยุทธ์การรักษาความปลอดภัยข้อมูลในเชิงรุกที่สามารถปรับเปลี่ยนได้มากขึ้น เมื่อโซลูชันที่ขับเคลื่อนด้วย AI ตรวจจับและประเมินความเสี่ยง การควบคุมการป้องกันแบบอัตโนมัติสามารถมีส่วนร่วมอย่างรวดเร็วเพื่อปกป้องข้อมูล โดยใช้การควบคุมการบรรเทาอย่างแม่นยำกับพื้นที่ที่มีความเสี่ยงสูง ตัวอย่างเช่น ในกรณีที่ผู้ใช้ที่มีความเสี่ยงสูงตรวจพบตัวบ่งชี้เริ่มต้นของความตั้งใจในการขโมยข้อมูล องค์กรสามารถใช้นโยบายการป้องกันข้อมูลสูญหาย (DLP) ที่เข้มงวดมากขึ้น เพื่อก้าวนำหน้าเหตุการณ์ด้านความปลอดภัยของข้อมูลในเชิงรุก

เราหวังว่าคุณจะได้รับข้อมูลเชิงลึกและคำแนะนำในรายงานนี้ที่มีประโยชน์ในการปรับปรุงสถานะการรักษาความปลอดภัยข้อมูล และเสริมความแข็งแกร่งให้กับองค์กรของคุณจากความเสี่ยงที่พัฒนาอยู่ตลอดเวลา

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับ Microsoft Data Security โปรดไปที่ https://aka.ms/DataSecurityNews

วัตถุประสงค์การวิจัย ระเบียบวิธี และการรับสมัครผู้ถูกสัมภาษณ์โดยละเอียด

วัตถุประสงค์ของการวิจัยประกอบด้วย:

1. ทำความเข้าใจภูมิทัศน์ด้านความปลอดภัยของข้อมูล รวมถึงลำดับความสำคัญ แนวความคิด และความท้าทาย
2. จัดทำแผนผังสาเหตุและผลกระทบของเหตุการณ์ด้านความปลอดภัยข้อมูล และระบุการดำเนินการที่ทีมรักษาความปลอดภัยข้อมูลสามารถทำได้เพื่อปรับปรุงมาตรการรักษาความปลอดภัยข้อมูล
3. สำรวจอนาคตของความปลอดภัยข้อมูล รวมถึงกลยุทธ์และนวัตกรรมใหม่ๆ เกี่ยวกับการใช้ AI เพื่อความปลอดภัยข้อมูล

วิธีการ:

แบบสำรวจออนไลน์ในหลายประเทศความยาว 15 นาที จัดทำขึ้นระหว่างวันที่ 28 กรกฎาคม – 9 สิงหาคม 2023 ในกลุ่มผู้มีอำนาจตัดสินใจด้านความปลอดภัยข้อมูล 822 ราย

คำถามที่มีศูนย์กลางอยู่ที่ภาพรวมความปลอดภัยข้อมูล วิธีที่ทีมรักษาความปลอดภัยข้อมูลจัดสรรทรัพยากร เหตุการณ์ด้านความปลอดภัยข้อมูล และทัศนคติต่อและการใช้ปัญญาประดิษฐ์ (AI) เพื่อความปลอดภัยข้อมูล

เพื่อให้เป็นไปตามเกณฑ์การคัดกรอง ผู้มีอำนาจตัดสินใจด้านความปลอดภัยจะต้อง:

CISO และผู้มีอำนาจตัดสินใจเหมือนกัน (C-2 ขึ้นไป) ที่มีหน้าที่ดูแลความปลอดภัยของข้อมูล

ทำงานที่องค์กรขนาดใหญ่ (พนักงานมากกว่า 500 คน หลากหลายขนาด)

การผสมผสานระหว่างอุตสาหกรรมที่ได้รับการควบคุมและไม่ได้รับการควบคุม (ไม่ใช่ทางการศึกษา ภาครัฐ หรือองค์กรไม่แสวงหาผลกำไร)

จากผู้มีอำนาจตัดสินใจด้านความปลอดภัยข้อมูล 822 รายที่ได้รับการสำรวจสำหรับการวิจัยนี้ ซึ่งแบ่งตามประเทศ ได้แก่:

US	329
สหราชอาณาจักร	322
ออสเตรเลีย	171